With effect from : 2019-20(R-19)

VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

9-5-81, Ibrahimbagh, Hyderbad-500031, Telangana State

DEPARTMENT OF MATHEMATICS

BASICS OF CRYPTOLOGY
(OPEN ELECTIVE)

for B.E., III – sem.,(CBCS)

(Common to all branches except for CSE)

Instruction: 2 Hours per week	Sem. End Exam Marks: 60	Subject Reference Code : U19OE310MA
Credits : 2	Sessional Marks: 40	Duration of Semester End Exam : 3 Hrs

COURSE OBJECTIVES	COURSE OUTCOMES
The course will enable the students to:	*At the end of the course students will be able to:*
1. **Study** fundamentals of number theory.	1. **Apply** the knowledge of Congruences for Modular exponentiation and solving Linear Congruences.
2. **Study** various methods under monoalphabetic substitution ciphers.	2. **Apply** the methods under monoalphabetic substitution ciphers to encipher and decipher.
3. **Understand** the methods under polyalphabetic substitution ciphers and public key cryptography.	3. **Apply** the methods under polyalphabetic substitution ciphers to encipher and decipher.
4. **Study** Public key Cryptography and Cryptographic protocols and algorithms.	4. **Apply** the methods RSA Cryptosystem.

UNIT- I (6 Hours)

Number Theory:

Divisibility- Euclidean Algorithm – GCD using Euclidean Algorithm –Introduction to Congruences -Modular Arithmetic –Fast Modular Exponentiation-Linear Congruences.

UNIT- II (6 Hours)

Monoalphabetic Substitution Ciphers:

Introduction to Cryptology and Basic Terminology -Monoalphabetic Substitution Ciphers-The Additive (or shift) Cipher –The Multiplicative Cipher - The Affine Cipher.

UNIT –III (8 Hours)

Polyalphabetic Substitution Ciphers :

Polyalphabetic Substitution Ciphers - Integer Matrices - The Hill Digraph Cipher - The Hill Trigraph Cipher - The Vigenère Square Cipher – The Playfair Cipher -The Permutation Cipher – The Exponentiation cipher

N. Vasudha.

(chairman, BOS)

UNIT –IV (6 Hours)

Public Key Cryptography :

Public Key Cryptography –RSA Cryptosystem- Knapsack Cipher.
Cryptographic Protocols & Applications – Diffie-Hellman Key Exchange.

Text Book:

Elementary Number Theory , Kenneth H. Rosen, Pearson India Education services Pvt.Ltd, 6th edition.

Reference Book :

A Course in Number Theory and Cryptography by Neal Koblitz, Springer, New York.

Online Resources:

1. https://onlinecourses.nptel.ac.in/noc16_cs21
2. www.mastermathmentor.com

(Prof. N. Kishan)
(OU Nominee)

(Prof. D.Srinivasacharya)
(Subject Expert -1)

ARamu
(Prof.A. Ramu)
(Subject Expert-2)

(Dr. B Srivathsa) 18.6.15
(Industry Expert)

N.Vasudha
(Dr.N Vasudha)
(Chairman)